预警编号：YJ-2017024

恒安嘉新

关于 DNSmasq 存在多个高危漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 10 月 11 日

1 漏洞描述

近期，互联网爆出 DNSmasq 多个安全漏洞（CVE-2017-14491、CVE-2017-14492、CVE-2017-14493、CVE-2017-14494、CVE-2017-14495、CVE-2017-14496、CVE-2017-13704），综合利用漏洞，远程攻击者可在目标系统上执行任意代码、造成服务崩溃或窃取内存敏感信息，影响范围涉及服务器、终端（包括移动终端）操作系统发行版本及相关组件，且当前利用方法已经公开，有可能诱发大规模攻击。漏洞危害程度为高危(High)。

2 影响范围

漏洞影响范围十分广泛，涉及 Linux 以及 Android 操作系统发行版本以及多个自身组件版本，也波及到一些网络设备或终端设备固件。

受影响的操作系统发行版本以及相关组件列表：

Ubuntu Ubuntu Linux 17.04

Ubuntu Ubuntu Linux 16.04 LTS

Ubuntu Ubuntu Linux 14.04 LTS

Thekelleys Dnsmasq 1.2.2

Thekelleys Dnsmasq 2.77

Thekelleys Dnsmasq 2.75

Thekelleys Dnsmasq 2.72

Thekelleys Dnsmasq 2.71

Thekelleys Dnsmasq 2.70

Thekelleys Dnsmasq 2.7

Thekelleys Dnsmasq 2.65

Thekelleys Dnsmasq 2.64

Thekelleys Dnsmasq 2.63

Thekelleys Dnsmasq 2.62

Thekelleys Dnsmasq 2.61

Thekelleys Dnsmasq 2.60

Thekelleys Dnsmasq 2.6

Thekelleys Dnsmasq 2.59

Thekelleys Dnsmasq 2.58

Thekelleys Dnsmasq 2.57

Thekelleys Dnsmasq 2.56

Thekelleys Dnsmasq 2.55

Thekelleys Dnsmasq 2.54

Thekelleys Dnsmasq 2.53

Thekelleys Dnsmasq 2.52

Thekelleys Dnsmasq 2.51

Thekelleys Dnsmasq 2.50

Thekelleys Dnsmasq 2.49

Thekelleys Dnsmasq 2.48

Thekelleys Dnsmasq 2.47

Thekelleys Dnsmasq 2.46

Thekelleys Dnsmasq 2.45

Thekelleys Dnsmasq 2.44

Thekelleys Dnsmasq 2.43

Thekelleys Dnsmasq 2.42

Thekelleys Dnsmasq 2.41

Thekelleys Dnsmasq 2.40

Thekelleys Dnsmasq 2.4

Thekelleys Dnsmasq 2.38

Thekelleys Dnsmasq 2.37

Thekelleys Dnsmasq 2.36

Thekelleys Dnsmasq 2.35

Thekelleys Dnsmasq 2.34

Thekelleys Dnsmasq 2.33

Thekelleys Dnsmasq 2.30

Thekelleys Dnsmasq 2.29

Thekelleys Dnsmasq 2.28

Thekelleys Dnsmasq 2.27

Thekelleys Dnsmasq 2.26

Thekelleys Dnsmasq 2.25

Thekelleys Dnsmasq 2.24

Thekelleys Dnsmasq 2.23

Thekelleys Dnsmasq 2.22

Thekelleys Dnsmasq 2.21

Thekelleys Dnsmasq 2.20

Thekelleys Dnsmasq 2.2

Thekelleys Dnsmasq 2.19

Thekelleys Dnsmasq 2.18

Thekelleys Dnsmasq 2.17

Thekelleys Dnsmasq 2.16

Thekelleys Dnsmasq 2.15

Thekelleys Dnsmasq 2.14

Thekelleys Dnsmasq 2.13

Thekelleys Dnsmasq 2.12

Thekelleys Dnsmasq 2.11

Thekelleys Dnsmasq 2.10

Thekelleys Dnsmasq 1.9

Thekelleys Dnsmasq 1.8

Thekelleys Dnsmasq 1.6

Thekelleys Dnsmasq 1.5

Thekelleys Dnsmasq 1.4

Thekelleys Dnsmasq 1.3

Thekelleys Dnsmasq 1.18

Thekelleys Dnsmasq 1.17

Thekelleys Dnsmasq 1.16

Thekelleys Dnsmasq 1.15

Thekelleys Dnsmasq 1.14

Thekelleys Dnsmasq 1.13

Thekelleys Dnsmasq 1.12

Thekelleys Dnsmasq 1.11

Thekelleys Dnsmasq 1.10

Thekelleys Dnsmasq 1.0

Thekelleys Dnsmasq 0.996

Thekelleys Dnsmasq 0.992

Thekelleys Dnsmasq 0.98

Thekelleys Dnsmasq 0.96

Thekelleys Dnsmasq 0.95

Thekelleys Dnsmasq 0.7

Thekelleys Dnsmasq 0.6

Thekelleys Dnsmasq 0.5

Thekelleys Dnsmasq 0.4

Slackware Slackware Linux 14.2

Slackware Slackware Linux 14.1

Slackware Slackware Linux 14.0

Slackware Slackware Linux 13.37

Slackware Slackware Linux 13.1

Slackware Slackware Linux 13.0

Redhat Enterprise Linux Workstation Optional 7

Redhat Enterprise Linux Workstation Optional 6

Redhat Enterprise Linux Workstation 7

Redhat Enterprise Linux Workstation 6

Redhat Enterprise Linux Server TUS 6.6

Redhat Enterprise Linux Server TUS 6.5

Redhat Enterprise Linux Server Optional EUS 7.3

Redhat Enterprise Linux Server Optional EUS 7.2

Redhat Enterprise Linux Server Optional EUS 6.5

Redhat Enterprise Linux Server Optional AUS 6.6

Redhat Enterprise Linux Server Optional AUS 6.5

Redhat Enterprise Linux Server Optional AUS 6.4

Redhat Enterprise Linux Server Optional 7

Redhat Enterprise Linux Server Optional 6

Redhat Enterprise Linux Server for ARM 7

Redhat Enterprise Linux Server EUS 7.3

Redhat Enterprise Linux Server EUS 7.2

Redhat Enterprise Linux Server AUS 6.6

Redhat Enterprise Linux Server AUS 6.5

Redhat Enterprise Linux Server AUS 6.4

Redhat Enterprise Linux Server AUS 6.2

Redhat Enterprise Linux Server - TUS 7.4

Redhat Enterprise Linux Server - TUS 7.3

Redhat Enterprise Linux Server - TUS 7.2

Redhat Enterprise Linux Server - Extended Update Support 7.4

Redhat Enterprise Linux Server - Extended Update Support 7.2

Redhat Enterprise Linux Server - Extended Update Suppor 7.3

Redhat Enterprise Linux Server - AUS 7.4

Redhat Enterprise Linux Server - AUS 7.3

Redhat Enterprise Linux Server - AUS 7.2

Redhat Enterprise Linux Server - 4 Year Extended Update Suppo rt 7.4

Redhat Enterprise Linux Server - 4 Year Extended Update Suppo rt 7.2

Redhat Enterprise Linux Server (for IBM Power LE) - 4 Year Exte nded Upd 7.3

Redhat Enterprise Linux Server (for IBM Power LE) - 4 Year Exte nded Update Support 7.4

Redhat Enterprise Linux Server 7

Redhat Enterprise Linux Server 6

Redhat Enterprise Linux Server 5

Redhat Enterprise Linux Long Life 5.9 server

Redhat Enterprise Linux HPC Node Optional 6

Redhat Enterprise Linux HPC Node 6

Redhat Enterprise Linux for Scientific Computing 7

Redhat Enterprise Linux for Power, little endian - Extended Upda te Supp 7.4

Redhat Enterprise Linux for Power, little endian 7

Redhat Enterprise Linux for Power, big endian - Extended Updat e Support 7.4

Redhat Enterprise Linux for Power, big endian 7

Redhat Enterprise Linux for Power little endian - Extended Upda te Suppo 7.3

Redhat Enterprise Linux for Power little endian - Extended Upda te Suppo 7.2

Redhat Enterprise Linux for Power big endian - Extended Updat e Support 7.3

Redhat Enterprise Linux for Power big endian - Extended Updat e Support 7.2

Redhat Enterprise Linux for IBM z Systems - Extended Update S upport 7.4

Redhat Enterprise Linux for IBM z Systems - Extended Update S upport 7.3

Redhat Enterprise Linux for IBM z Systems - Extended Update S upport 7.2

Redhat Enterprise Linux for IBM z Systems 7

Redhat Enterprise Linux EUS Compute Node 7.4

Redhat Enterprise Linux EUS Compute Node 7.3

Redhat Enterprise Linux EUS Compute Node 7.2

Redhat Enterprise Linux Desktop Optional 6

Redhat Enterprise Linux Desktop 7

Redhat Enterprise Linux Desktop 6

Redhat Enterprise Linux ComputeNode Optional EUS 7.3

Redhat Enterprise Linux ComputeNode Optional EUS 7.2

Redhat Enterprise Linux ComputeNode Optional 7

Redhat Enterprise Linux ComputeNode EUS 7.3

Redhat Enterprise Linux ComputeNode EUS 7.2

Redhat Enterprise Linux ComputeNode 7

Oracle Linux 7

Oracle Linux 6

openSUSE Leap 42.3

openSUSE Leap 42.2

Kubernetes Kubernetes 1.7.6

Kubernetes Kubernetes 1.7

Kubernetes Kubernetes 1.6.10

Kubernetes Kubernetes 1.6

Kubernetes Kubernetes 1.5.7

Kubernetes Kubernetes 1.5

Kubernetes Kubernetes 1.2

Google Android 7.1.1

Google Android 6.0.1

Google Android 5.1.1

Google Android 5.0.2

Google Android 4.4.4

Google Android 8.0

Google Android 7.1.2

Google Android 7.0

Google Android 6.0

Fedoraproject Fedora 27

Debian Linux 6.0 sparc

Debian Linux 6.0 s/390

Debian Linux 6.0 powerpc

Debian Linux 6.0 mips

Debian Linux 6.0 ia-64

Debian Linux 6.0 ia-32

Debian Linux 6.0 ia-30

Debian Linux 6.0 arm

Debian Linux 6.0 amd64

CentOS CentOS 7

CentOS CentOS 6

3 漏洞原理

DNSmasq 是一款广泛使用的开源软件，提供 DNS、DHCP、路由器广告和网络引导服务。在 DNS 服务中，DNSmasq 可以通过缓存 DNS 请求来提高对访问过的网址的连接速度；在 DHCP 服务，DNSmasq 可以用于为局域网电脑分配内网 ip 地址和提供路由。它还被广泛用于智能手机和便携式热点，并支持虚拟化框架中的虚拟网络。支持的平台包括 Linux(与 glibc 和 uclibc)、Andr oid、* BSD 和 Mac OS x。Dnsmasq 包含在大多数 Linux 发行版和 FreeBSD、OpenBSD 和 NetBSD 的端口系统中。此外，Dnsmasq 对 IPv6 网络也提供了完整支持。

近日互联网爆出某安全研究人员发现 Dnsmasq 存在的 7 个高危漏洞 ,相关漏洞详情如下：

1.CVE-2017-14491 远程攻击者可以通过发送特制的 DNS 数据包来触发堆溢出，并在目标系统上执行任意代码。

2、CVE-2017-14492 远程攻击者可以通过发送特制的 IPv6 路由器公告(RA ）消息来触发堆溢出，并在目标系统上执行任意代码。

系统使用：enable-ra,ra-only,slaac,ra-names, ra-advrouter, ra-stateless 等配置选项才会受到漏洞影响。

3.CVE-2017-14493 远程攻 击者可以通过发送一个专门设计的 DHCPv6 请求，以触发堆栈溢出并在目标系统上执行任意代码。

4.CVE-2017-14494 远程攻击者可以通过发送专门设计的 DHCPv6 包，以

触发 DHCPv6 中继代码中的一个缺陷，并从目标系统的进程内存中获取潜在的敏感信息。

5.CVE-2017-14495 远程攻击者可以发送特制的 DNS 数据包使 add_pseudoheader()函数分配的内存没有释放，在目标系统上的过度的消耗内存，导致拒绝服务。

6.CVE-2017-14496 远程攻击者可以通过发送专门的 DNS 数据包，以触发在 EDNS0 代码中的一个整数下溢和随后的缓冲区溢出错误，并导致目标服务崩溃。

系统使用：add-mac、add-cpe-id、add-subnet 等配置选项才会受到漏洞的影响。

7.CVE-2017-13704 因在 2.77 版本中的安全修补程序存在回归错误，远程攻击者可以通过发送特制的 DNS 查询以导致目标服务崩溃。

上述漏洞可以通过 DNS 和 DHCP 协议远程触发，在特定情况下，攻击者通过构造特定数据包请求，导致远程代码执行、信息泄露和拒绝服务。

4 修复建议

DNSmasq 2.78 版本已修复了这些漏洞，建议用户可通过链接自行更新：http://www.thekelleys.org.uk/dnsmasq/

如未能更新，可以采用以下临时解决方案：

1. 必要情况下，请关闭影响 DNSmasq 安全的配置选项；
2. 使用白名单机制，这样可以使 DNSmasq 服务限制访问权限；
3. 使用可信的 DNS 服务。